National Science Foundation

NSF Personnel Security System and NSF Photo Identification Card System

Privacy Impact Assessment

Version: 1

Date: 10/19/2005

Table of Contents

Revisions

Revision Number	Author	Date	Description

1. BACKGROUND

The Privacy Impact Assessment (PIA) is a vehicle to address privacy issues in information systems. The PIA template establishes requirements for addressing privacy during the information systems development process; it defines and documents the privacy issues a project must address and outline; and serves as part of the Certification and Accreditation (C&A) process for a NSF General Support System (GSS) or a Major Application (MA).

Privacy issues addressed by this assessment include:

1. The use of the information must be controlled.
2. Information may be used only for a necessary and lawful purpose.
3. Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them.
4. Information collected for a particular purpose should not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
5. Any information used must be sufficiently accurate, relevant, timely and complete to assure fair treatment of the individual.

Homeland Security Presidential Directive 12 (HSPD-12) requires improved processes to strengthen Personal Identity Verification (PIV) of all Federal employees and contractors. National Institute of Standards and Technology's (NIST) Federal Information Processing Standards Publication 201 (FIPS 201) provides implementation guidance for HSPD-12.

HSPD-12 emphasizes the need to protect privacy of Government employees and contractors. The HSPD-12 requirements for privacy and security controls include:

1. Naming a Senior Agency Official for Privacy (i.e., the NSF CIO) to oversee the privacy protections related to implementation of the Personal Identity Verification (PIV) process.
2. Publishing a Privacy Act statement available to all employees and contractors.
3. Conducting a Privacy Impact Assessment (PIA) of the systems that support the PIV process. This must be submitted to OMB Privacy Officials for review.
4. Publishing a Privacy Act System of Records Notice in the Federal Register, for public comment (revision to follow when needed).

1.1 Organizational Background

At NSF, the Divisions of Human Resources Management (HRM) and Administrative Services (DAS) have the lead with the HSPD-12 requirements related to physical access (to buildings and office space). In the PIV process, HRM authorizes the issuance of ID cards by examining identity source documents and completing and adjudicating required background investigations. DAS issues the cards to authorized Applicants and manages the card life cycle. HRM is responsible for NSF's Personnel Security System of Records (SOR) (NSF-26), while DAS is responsible for the NSF Photo Identification Card SOR (NSF-66).

2. SCOPE

Protecting an individual's right to privacy is predicated on various Federal laws, directives, and standards; the overarching Federal laws being the Privacy Act of 1974 and the more recent E-Government Act of 2002. Federal guidance requires that, where possible, the PIA process be integrated into the system life cycle. Therefore, this PIA is base-lined using instruction from NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle* and other Federal guidance.

3. ENVIRONMENT

A critical component of completing the C&A process is categorizing the information type(s) that the system processes. An information type is defined as "*a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation*[1]." Some NSF systems process privacy information. Thus, this PIA serves to determine to what extent this privacy information must be adequately protected.

The operational environment for the NSF Photo Identification Card System (NSF-66) consists of a standalone personal computer-based security system, C-Cure 800. The system consists of a server, photo and signature capture and input devices, and connections to NSF's card readers located throughout the building. The system is used for card issuance and management. The server is in a highly secure building location in a locked room and is password-protected. The server is not connected to other NSF systems, including the LAN and Intranet. Communication among Administrative Officers (AOs), HRM and DAS (as documented in the standard operating procedures) is generally handled through regular email. Social Security Number is not included in this system and therefore is not transmitted via email.

The operational environment for the NSF Personnel Security System (NSF-26) consists of a limited access, password protected database. Only the Personnel Security Officer (Chief of the Employee Relations Branch, HRM) and the Personnel Security Specialist have access to the database. The database is populated with names, dates and other data (see response to Section 4.1, question 1) by the system administrators as investigations are requested and adjudicated. Information from the database is released on a need-to-know basis as identified in the System of Records Notice. In addition, the database is used to confirm and track the procedural steps and dates (e.g., NACI initiated on [date]) for an employee or contractor to receive an ID card.

4. PRIVACY IMPACT ASSESSMENT CRITERIA

The following sections contain the appropriate questions that are used to collect the required information. The NSF Privacy Officer and other reviewing officials will analyze the results to ensure that an individual's personally identifiable information is adequately secure. The

[1] FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004, Section 3, page 1.

completed PIA will be forwarded to the appropriate individuals for review, signature, and approval.

4.1 Data in the System

The sources of the system information are an important privacy consideration. The information becomes especially important if the data is gathered from other than NSF records. Information collected from non-NSF sources should be verified, to the extent practicable, for accuracy, that the information is current, and the information is complete. Accurate information is important if the information will be used to make determinations about individuals.

Privacy Criteria	Descriptive Response
1. Provide a general description of the information type (i.e., person's name, SSN, etc.) to be collected or processed by the GSS or MA or reference *the NSF Information Categorization and Sensitivity Assessment.*	NSF- 26 – Individual's name; SSN; date of birth (DOB); place of birth (POB); Directorate; Division; entry on duty date (EOD); Position Sensitivity; and Type of Appointment Investigation Information – Type; Date Requested; Date Completed; Clearance Level; Source of Inquiry Code; Amount; Miscellaneous Obligation Record (MOR) #; OPM # NSF-66 – Individual's name (last, first and MI); employment status (permanent employee, contractor, IPA, temporary employee, guest, Child Development Center staff or non-NSF parent or guardian of children in the CDC); digital photograph; digitized signature; unique proximity card number; not to exceed (NTE) date; special access clearances (e.g., access to Stafford Place II) requested by AO; card reader(s) accessed and date/time of access
2. What are the sources of the information in the system? (Note: This is an important privacy consideration if the data is gathered from other than NSF records).	NSF-26 – Applicant and HRM Security Personnel NSF-66 – Applicant, HRM and AO provide personal and employment information; access information is captured automatically by card readers
3. What NSF files and databases are used?	NSF-26 – Access data base; e-mails and paper files NSF-66 – C-Cure 800 card management/security system and email messages
4. What other Federal Agencies, if any, are providing data for use in the system?	NSF-26 – OPM NSF-66 – N/A

Privacy Criteria	Descriptive Response
5. From what other third party sources will data be collected?	NSF-26 – N/A NSF-66 – N/A
6. What information will be collected from the employee?	NSF-26 – Primarily individual's name, DOB, POB NSF-66 – Primarily individual's name (last, first and MI); digital photograph; and digitized signature
7. If data is collected from sources other than NSF records, how is it being verified for accuracy? *(Note: This is especially important if the information will be used to make determinations about individuals).*	NSF-26 – Visual check of photo ID NSF-66 – N/A
8. How will data be checked for completeness?	NSF-26 – N/A NSF-66 – Data are checked through report generation
9. Is the data current? How do you know? What mechanisms were used to validate the data's currency?	NSF-26 – Information is collected directly from the employee/contractor as they enter on duty NSF-66 – Information is collected directly from the employee/contractor as they enter on duty. Information about employee/contractor entry into NSF space is captured automatically in real time by card readers.
10. What data elements are described? What level of detail is used in documenting data elements?	NSF-26 – N/A NSF-66 – See response to question #1 above
11. If data elements are documented, what is the name of the document?	NSF-26 – N/A NSF-66 – N/A

4.2 Access to the Data

Who has access to the data in a system must be defined and documented. Users of the data can be individuals, other systems, and other agencies. Individuals who have access to the data can be system users, system administrators, system owners, managers, and developers. When individuals are granted access to a system, their access should be limited, where possible, to only that data needed to perform their assigned duties. If individuals are granted access to all of the data in a system, procedures need to be in place to deter and detect browsing and unauthorized access. Other systems are any programs or projects that interface with the system and have access to the data.

Privacy Criteria	Descriptive Response

Privacy Criteria	Descriptive Response
1. Who has access to the data in the system? (Note: Users of the data can be individuals, other systems, programs, projects, or other agencies. Individuals who have access to the data can be system users, system administrators, system owners, managers, and developers).	NSF-26 – The Employee Relations Branch (ERB) of the Division of Human Resource Management (HRM). System administrators are the Chief, ERB (who is the Personnel Security Officer) and the Personnel Security Specialist. NSF-66 – Access is restricted to a small group of internal users whose duties involve physical security and who have been trained to recognize what is considered proper access. The Facilities and Operations Branch (FOB) of the Division of Administrative Services (DAS) is the system owner. System administrators are the Head, Facilities Management Section (FMS), FOB; and two members of Building Services. These individuals, along with one member of the Project Management Unit, FMS, are the system users. The Chief, FOB, does not have access to the database but has access to the NSF-ID-Badge email alias, which is used to coordinate badge issuance procedures (such as requesting ID badges).
2. Where individuals are granted access to all of the data in a system, what procedures are in place to deter and detect browsing and unauthorized access?	NSF-26 – Access to information is controlled by password and in a room that is locked at all times when not in use. NSF-66 – Access to information on a standalone computer is controlled by password and in a room that is locked at all times when not in use. Authorized users have access to all data in the system in accordance with their position duties. Users are trained to know what is considered to be proper access.
3. When individuals are granted access to a system, how is their access being limited, where possible, to only that data needed to perform their assigned duties?	NSF-26 – See questions 1 and 2 above NSF-66 – See questions 1 and 2 above
4. How or what tools are used to determine a user's data access?	NSF-26 – Access is restricted by job functions and the use of user IDs/passwords. Authorized users need access to the set of data contained in the system as described in Section 4.1, question 1. NSF-66 – Access is restricted by job functions and the use of user IDs/passwords. All authorized

Privacy Criteria	Descriptive Response
	users need access to the set of data contained in the system as described in Section 4.1, question 1.
5. Describe the criteria, the procedures, the controls, and the responsibilities in place regarding the manner in which data access is documented.	NSF-26 – N/A NSF-66 – The C-Cure 800 security system automatically documents data access. Standard operating procedures govern system access.
6. Do other systems share data or have access to data in this system? If yes, explain.	NSF-26 – No NSF-66 – No
7. Who has the responsibility for protecting the privacy rights of the individuals affected by any system interface?	NSF-26 – N/A NSF-66 – DAS and HRM are responsible for protecting the privacy rights of the individuals affected by any system interface.
8. Will other agencies share data or have access to data in this system?	NSF-26 – No NSF-66 – No
9. How will the NSF use this data?	NSF-26 – To track information on personnel security clearances, and investigations. NSF-66 – To produce photo identification cards (proximity cards) for access to the building as well as for building security; to identify the bearer of the card as a Federal employee or contractor; to change access permissions on cards; and to track stolen or lost cards
10. Who is responsible for assuring proper use of the data?	NSF-26 – The system owners NSF-66 – The system owner
11. How will the system ensure that agencies only get the information they are entitled to?	NSF-26 – N/A NSF-66 – External agencies do not have access to this NSF data.

4.3 Attributes of the Data

When requirements for the data to be used in the system are being determined, those requirements must include the privacy attributes of the data. The privacy attributes are derived from the legal requirements imposed by the Privacy Act of 1974. First, the data must be *relevant and necessary* to accomplish the purpose of the system. Second, the data must be *complete, accurate and timely*. It is important to ensure the data has these privacy attributes in order to assure fairness to the individual in making decisions based on the data.

Privacy Criteria	Descriptive Response
1. Explain how the use of the data is both relevant and necessary to the purpose for which the system is being designed?	NSF-26 – The Personnel Security System tracks information on Personnel security clearances and investigations. This information is necessary in order to clear the employee or contractor for the issuance of PIV card/ID badge, which allows access to buildings/space. The PIV card is a requirement for Federal employment, as well as a requirement for all contractors (on-site more than 6 months). NSF-66 – The PIV card/ID badge supports internal operations, i.e., physical access to buildings/space. The PIV card (and the processes leading up to it) are a requirement for Federal employment, as well as being required for all contractors (on-site more than 6 months).
2. Will the system derive new data or create previously unavailable data about an individual through aggregation for the information collected?	NSF-26 – No NSF-66 – No
3. Will the new data be placed in the individual's record?	NSF-26 – N/A NSF-66 – No
4. Can the system make determinations that would not be possible without the new data?	NSF-26 – N/A NSF-66 – N/A
5. How will the new data be verified for relevance and accuracy?	NSF-26 – N/A NSF-66 – N/A
6. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	NSF-26 – limited access, password protected database. NSF-66 – N/A
7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain	NSF-26 – The database record can be verified by OPM, Office of Investigations. NSF-66 – N/A
8. How will the data be retrieved? Can the data be retrieved using a personal identifier (i.e., name, address, etc.)? If yes, explain.	NSF-26 – Data can be retrieved electronically by last name in order to relay data to PIV issuers, Security Officers at other agencies, a court or litigation authority, DOJ and other investigative

Privacy Criteria	Descriptive Response
	entities. NSF-66 – Data can be retrieved by name, by card number and by card access point. Retrieval is necessary to make changes to the card's permissions, to extend NTE dates, to deactivate/revoke cards, to provide reports to investigative bodies such as OIG, etc.
9. What are the potential effects on the due process rights of individuals with respect to the following: • Consolidation and linkage of files and systems; • Derivation of data; • Accelerated information processing and decision-making; • Use of new technologies?	 N/A N/A N/A N/A
10. How will these affects be mitigated?	NSF-26 – N/A NSF-66 – N/A

4.4 Maintenance of Administrative Controls

Automation of systems can lead to the consolidation of processes, data, and the controls in place to protect the data. When administrative controls are consolidated, they should be evaluated so that all necessary controls remain in place to the degree necessary to continue to control access to and use of the data.

Data retention procedures should be documented. Data retention procedures require review to ensure they meet statutory requirements. Rules must be established for the length of time information is kept and for assuring that it is properly eliminated (i.e., archived, deleted, etc.) at the end of that time.

The intended and potential monitoring capabilities of a system must be defined and safeguards must be installed to ensure privacy and prevent unnecessary intrusion.

Privacy Criteria	Descriptive Response
1. Explain how the system and its use will ensure equitable treatment of individuals.	NSF-26 – The information is used only in connection with tracking clearances and investigations and is only disclosed to individuals with a bona fide need to know NSF-66 – The information is used only in

Privacy Criteria	Descriptive Response
	connection with card management and is only disclosed to individuals with a bona fide need to know
2. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?	The system is only operated at NSF's headquarters location in Arlington, VA
3. Explain any possibilities of disparate treatment of individuals or groups.	None
4. What are the retention periods of data in this system?	NSF-26 – Data are maintained during the course of employment (i.e., requirement for physical access to NSF space). Data are retained for 2 years after employee/contractor separation. NSF-66 – Data are maintained during the course of employment (i.e., requirement for physical access to NSF space). Data are retained up to 90 days after employee/contractor separation, NTE date or card revocation; then the data are deleted.
5. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	NSF-26 – Data are electronically eliminated by system administrators NSF-66 – Standard operating procedures have been developed and documented
6. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	NSF-26 – Access database is backed up twice monthly. NSF-66 – Employees can review and update their personal information as needed. C-Cure database is backed up twice monthly and data are stored at a secure off-site location. The database back up system is tested twice yearly to ensure data integrity and availability. Building Services staff review the DIS list of LAN/email IDs every 60 days to determine that ID Badges are still required by contractors, to ensure currency of data. Discrepancies are resolved with AOs and Sponsors. The Contractor confirms the continuing need for ID Badges for the Contractor's employees through regular reports.
7. Is the system using technologies in ways that NSF has not previously employed? How does the use of this technology affect	NSF-26 – No. This is a standalone system. The technology used in this application is not networked and adds no risk of harm to individual

Privacy Criteria	Descriptive Response
individual's privacy?	privacy. NSF-66 – No. This is a standalone system. The technology used in this application is not networked and adds no risk of harm to individual privacy.
8. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	NSF-26 – No NSF-66 – The system records which card readers at NSF are accessed (for purposes of entrance into NSF space only) by each card and the date and time of entrance.
9. Will this system provide the capability to identify, locate and monitor groups of people? If yes explain.	NSF-26 – No NSF-66 – Data can be retrieved by access point, making it possible to determine that group of users who used the access point in a given time period.
10. What controls will be used to prevent unauthorized monitoring?	NSF-26 – Only authorized users can access the information and provide it to authorities with a need to know. NSF-66 – Only authorized users can access the information and provide it to authorities with a need to know.
11. Under which System of Record notice does the system operate? Provide number and name.	NSF-26 – Personnel Security NSF-66 – NSF Photo Identification Card System
12. If the system is being modified, will the System of Record require amendment or revision? Explain	NSF-26 – No NSF-66 – The System of Records Notice (SORN) does not need revision at this time but will be revised as PIV implementation continues in FY 2006.

Additional Assistance

For additional assistance with completing this assessment, you may contact Division of Information Systems Security Officer at 703-292-8341.

Review Authority

Ensure that the appropriate signatures are documented prior to forwarding to the NSF Privacy Officer

NSF Privacy Act Officer

Date: _____Name: _____

Comments:

HRM Program Manager Review

Date: _____Name:_____

Comments:

DAS Program Manager Review

Date: _____Name: _____

Comments:

HRM System Owner Review

Date: _____Name: _____

Comments:

DAS System Owner Review

Date: _____Name: _____

Comments: